AMENDMENTS TO THE CLAIMS

1-18. (Cancelled)

19. (Currently Amended) Apparatus for ensuring the integrity of an application executed on a computer having data storage arranged sectorwise, comprising:

apparatus for learning about ~~the~~ permitted ~~normal~~ access behavior of said application to said data storage arranged sectorwise by monitoring accesses of said application to sectors ~~elements~~ of said data storage during a limited learning period in which said application is assumed to be uninfected by a virus; and

an enforcement device, operative after said limited learning period is over, for identifying and preventing said application from accessing sectors ~~elements~~ of data storage that do not correspond with the permitted access ~~normal~~ behavior of said application.

20. (Cancelled)

21. (Currently Amended) Apparatus according to claim 19 wherein said enforcement device is operative to prompt a user to give specific permission, upon occurrence of an attempt of said application ~~the program~~ to access sectors of data storage ~~files~~ not accessed during said limited learning period.

22-24. (Cancelled)

25. (Currently Amended) A method for detecting forbidden ~~abnormal~~ behavior of a first application executed on a computer system, and preventing ~~the~~ damage thereupon, comprising:

monitoring accesses of said first application to sectors ~~elements~~ of data storage arranged sectorwise in a storage device over a limited learning period, in which said first application is assumed to be uninfected by a virus, ~~of time~~ and storing data storage access permission information about said accesses in an enforcement file, thereby

learning ~~the~~ permitted access ~~normal~~ behavior of said application; and

when said limited learning period is over, detecting attempts of said application to access sectors ~~elements~~ of data storage that do not correspond to said permitted access ~~normal~~ behavior as determined by said enforcement file and inhibiting said attempts ~~accesses~~, thereby preventing ~~the~~ damage thereupon.

26. (Currently Amended) A method according to claim 25, further comprising enabling a ~~the~~ user of said first application to determine said permitted access ~~normal~~ behavior during said limited learning period.

27. (Currently Amended) A method according to claim 25, further comprising enabling a ~~the~~ user of said first application to determine said permitted access ~~normal~~ behavior after said limited learning period is over.

28. (Currently Amended) A method according to claim 26, further comprising enabling the user of said first application to determine said permitted access ~~normal~~ behavior after said limited learning period is over.

29. (Currently Amended) A method according to claim 25, further comprising detecting attempts of a child ~~daughter~~ application of said first application to access sectors ~~elements~~ of data storage that do not correspond to said permitted access ~~normal~~ behavior as determined by said enforcement file and inhibiting said attempts ~~accesses~~, thereby preventing ~~the~~ damage thereupon.

30. (Currently Amended) A method according to claim 26, further comprising detecting attempts of a child ~~daughter~~ application of said first application to access sectors ~~elements~~ of data storage that do not correspond to said permitted access ~~normal~~ behavior as determined by said enforcement file and inhibiting said attempts ~~accesses~~, thereby preventing ~~the~~ damage thereupon.

31. (Currently Amended) A method according to claim 27, further comprising detecting

attempts of a child ~~daughter~~ application of said first application to access sectors ~~elements~~ of data storage that do not correspond to said permitted access ~~normal~~ behavior as determined by said enforcement file and inhibiting said attempts ~~accesses~~, thereby preventing ~~the~~ damage thereupon.

32. (Currently Amended) A method according to claim 25, further comprising detecting attempts of a second application to access sectors ~~elements~~ of data storage that do not correspond to said permitted access ~~normal~~ behavior as determined by said enforcement file and inhibiting said attempts ~~accesses~~, thereby preventing ~~the~~ damage thereupon.

33. (Currently Amended) A method according to claim 26, further comprising detecting attempts of a second application to access sectors ~~elements~~ of data storage that do not correspond to said permitted access ~~normal~~ behavior as determined by said enforcement file and inhibiting said attempts ~~accesses~~, thereby preventing ~~the~~ damage thereupon.

34. (Currently Amended) A method according to claim 27, further comprising detecting attempts of a second application to access sectors ~~elements~~ of data storage that do not correspond to said permitted access ~~normal~~ behavior as determined by said enforcement file and inhibiting said attempts ~~accesses~~, thereby preventing ~~the~~ damage thereupon.

35. (Currently Amended) A method according to claim 32 ~~claim 29~~, wherein said second application is executed on a second computer.

36. (Currently Amended) The apparatus of claim 19, wherein only permitted ~~normal~~ accesses of said application to sectors ~~elements~~ of said data storage are monitored during said limited learning ~~time~~ period.

37-38. (Cancelled)

39. (Currently Amended) A method according to claim 25, wherein said monitoring ~~of~~ ~~said~~ accesses of said first application to sectors ~~elements~~ of data storage learns only the

permitted access ~~normal~~ behavior of said first application.

40. (Currently Amended) Apparatus for ensuring the integrity of an application executed on a computer having data storage arranged sectorwise, comprising:

apparatus for learning about ~~the~~ permitted ~~normal~~ access behavior of said application to said data storage arranged sectorwise by monitoring accesses of said application to sectors ~~elements~~ of said data storage during a limited learning period in which said application is assumed to be uninfected by a virus; and

an enforcement device, operative after said limited learning period is over, for granting said application no access rights to any sectors ~~elements~~ of data storage other than those sectors ~~elements~~ accessed during said limited learning period, to which access will be allowed.

41. (Currently Amended) A method for allowing permitted access and blocking forbidden access ~~detecting abnormal~~ behavior of a first application executed on a computer system~~, and preventing the damage thereupon,~~ comprising:

monitoring accesses of said application to sectors ~~elements~~ of data storage arranged sectorwise in a storage device over a limited learning period, in which said first application is assumed to be uninfected by a virus, ~~of time~~ and storing data storage access permission information about said accesses in an enforcement file, thereby learning ~~the~~ permitted access ~~normal~~ behavior of said application; and

when said limited learning period is over, granting said application no access rights to any sectors ~~elements~~ of data storage other than those sectors ~~elements~~ accessed during said limited learning period, to which access will be allowed.

42. (Currently Amended) A method for blocking forbidden ~~ensuring normal~~ access behavior of a program, the method comprising the steps of:

providing a list of access permissions of said program to sectors ~~elements~~ of data storage, whereby access of said program to sectors of data storage not on said list are forbidden accesses;

monitoring access requests of said program to data storage; and

upon indicating a request to access a sector ~~an element~~ of data storage which does not comply with said list, blocking said request ~~attempt~~.

43. (Currently Amended) A method according to claim 42, further comprising:

during a limited learning period in which said program is assumed to be uninfected by a virus, upon indicating by said monitoring a request to access a sector ~~an element~~ of data storage which is not on said list, adding said sector ~~element~~ to said list as allowable for access.

44. (Currently Amended) A method according to claim 42, wherein said monitoring further includes requests of a child ~~daughter~~ application of said program to access data storage.

45. (New) Apparatus according to claim 19 wherein said data storage arranged sectorwise is selected from a group consisting of a path and a file.

46. (New) A method according to claim 25, wherein said data storage arranged sectorwise is selected from a group consisting of a path and a file.

47. (New) Apparatus according to claim 40 wherein said data storage arranged sectorwise is selected from a group consisting of a path and a file.

48. (New) A method according to claim 41, wherein said data storage arranged sectorwise is selected from a group consisting of a path and a file.